Collection of ADC

2132. SHRI NILOTPAL BASU: Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) how much Access Deficit Charge has been collected against the target since its inception till date, year-wise; and

(b) the relative amounts contributed through various types of calls-STD, ISD and others?

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (DR. SHAKEELAHMAD): (a) and (b) Bharat Sanchar Nigam Limited (BSNL) was not measuring Intra Network minutes that would be required for computing the amount of intra network Access Deficit Charge (ADC) retained by BSNL. Therefore, the exact amount of ADC collected against the target since its inception including through various types of calls-STD, ISD is not maintained.

Increase in cyber crimes

2133. SHRIMATI S.G. INDIRA: Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether it is a fact that the country has been witnessing increase in cyber crimes;

(b) if so, the details thereof;

(c) whether Government have set up any committee to probe the issues concerning cyber crimes;

(d) if so, the details thereof;

(e) whether Government have made any agreement with foreign countries to deal with cyber crimes committed on foreign lands but affecting India; and

(f) if so, the details thereof?

THE MINISTER OF STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (DR. SHAKEELAHMAD): (a) and (b) The cases registered under cyber crimes in States/Union Territories in

India during the last three years, as per the report of the National Crime Records Bureau (NCRB), are as follows:

Year	Crimes Registered under IT Act	Crimes Registered Under IPC	Total
2002	70	738	808
2003	60	411	471
2004	68	279	347

The cyber crime figures from the Cyber Crime Investigation Cell/CBI for the last three years are as follows:

Year	No. of Cases
2003	3
2004	1
2005	5

The above figures show a mixed trend for crimes under IT Act and a declining trend for crimes under relevant IPC Sections.

(c) and (d) The Department of Information Technology had set up an Expert Committee under the Chairmanship of Secretary, Department of Information Technology to review the existing provisions in the Information Technology Act, 2000. Some of the important cyber crime issues considered by the Expert Committee related to Child Pornography, Video Voyeurism, Digital Evidence Examiners, Data Privacy, E-Commerce Frauds, Phishing and Frauds on Online Auction Sites. The salient recommendations of the Expert Committee are given in the enclosed Statement (*See* below).

(e) and (f) Cyber Crimes Cases are covered under Mutual Legal Assistance Treaties (MLATs) signed by India with other countries. Mutual need based cooperation of foreign countries is secured in this regard under the said Treaties. Besides, India is a member of Cyber Crime Technology Information Network System (CTINS), which is a Japanese Government initiative for mutual exchange of information regarding Cyber Crimes among the member countries which is advisory in nature.

Statement

Summary of the recommendations of the Expert Committee

1. As the technologies and applications in IT sector change very rapidly, some of the provisions related to parameters that may change from time to time have been suggested to provide for the new developments to be incorporated by changes in rules/Government notifications. This would enable the law to be amended and approved much faster and would keep our laws in line with the changing technological environment.

2. In view of changing needs, operation of the Sub-section 4 of Section 1 may be made more flexible through prescription of such exception by rules rather than being part of the main Act.

3. The Committee has restructured several provisions in relation to recognition of Digital signatures, e-governance, penalties and adjudication. The suggestion is to make the Information Technology Act technically natural with minimum change in the IT Act, 2000. The amendment have been suggested in Section 4 of the Act to provide for electronic signature. With digital signature as one of the types of electronic signature and by enabling the detail of other form of electronic signature to be provided in the rules to be notified by the Central Government from time to time. This is enabling provision for Central Government to exercise as to when the technology other than digital signature matures.

4. The Committee has revisited Section 43, 65, 66, 67, 72 and 79 to focus issues pertaining to data protection and privacy so as to enable healthy business environment. The stringent provisions have been suggested in the Section. Proposals at Section 43 (ii) related to enabling of sensitive personnel with reasonable security proposals and procedures thereto have been recommended. The amendments have been suggested in Section 72 pertaining to breach of confidentiality and privacy. A new Sub-section as 72(ii) has been suggested to prevent intermidiaries to disclose information relating to user without his consent.

5. The Section 72 pertaining to breach of confidentiality have been redefined. The report of the Expert Committee seeks to address the

new phenomenon of video voyeurism, including transmission of MMS clips, the images of private areas of individuals without knowledge and its transmission without their consent. The new sub-Section has been proposed in Section 72 of the IT Act, 2000.

6. Amendment have been recommended in Section 69 of the IT Act, 2000 relating to the power to issue protection for inspection and monitoring any information through computer resource to take care of the concerns expressed by Ministry of Home Affairs.

7. In line with the Indian Penal Code, the Expert Committee has advocated classifications of Cyber Laws in cognizable and non-cognizable accordingly. Language of Section 66 related to computer related offences may be revised to be in lines with Section 43 related to penalty for damage to computer resource. These have been graded with less degree of severity of offence when done by any person, dishonestly or fraudulently without the permission of the owner.

8. Section 67 related to Obscenity in electronic form has been revised to bring in line with IPC and other laws but fine has been increased because of ease of such operation in electronic form; link up with Section 79 w.r.t. liability of intermediary in certain cases has been provided.

9. A new section on section 67(2) has been suggested to address child pornography with higher punishment, a globally accepted offence.

10. A new section 68(1) has been proposed for providing modes and methods for encryption for secure use of the electronic medium, as recommended by earlier Inter Ministerial Working Group on Cyber Laws & Cyber Forensics (IMWG).

11. A new Section 78 A (Examiners of Electronic Evidence) may be added to notify the examiners of electronic evidence by the Central Government. This will help the Judiciary/Adjudicating officers in handling technical issues.

12. Section 79 has been revised to bring-out explicitly the extent of liability of intermediary in certain cases. EU Directive on E-Commerce 2000/31/EC issued on June 8th 2000 has been used as guiding principles. Power to make rules w.r.t. the functioning of the "Intermediary" including "Cyber Cafes" has been provided for under Section 87.